A PROBLEM OF DICKSON

By L. Carlitz

1. Let $p > 2$, $n \geq 1$. In 1909 Dickson [4] studied homogeneous polynomials $Q(x, y)$ with coefficients in $GF(p^n)$ such that $Q(a, b)$ is a non-zero square of the field for all (a, b) except $(0, 0)$ of the field; he called such forms definite. It follows from the definition that $Q(x, y)$ is of even degree. Dickson conjectured that every definite binary form of degree $2r$, $r > 1$, is a square provided p^n exceeds a certain bound N_r.

The writer showed [2] that this conjecture is correct and is a consequence of the Riemann hypothesis for the Artin zeta function; this hypothesis was proved by A. Weil [6]. Indeed a slightly stronger result was proved by considering polynomials $F(x)$ of arbitrary degree k rather than forms $Q(x, y)$ of even degree. Under the assumption that $F(a)$ is a non-zero square of $GF(p^n)$ for all a in $GF(p^n)$ it was shown that $F(x) = H^2(x)$, where $H(x) \in GF[p^n, x]$, provided $p^n > N_k$; the explicit bound $N_k = (k-1)^2$ suffices.

The purpose of the present note is to show in the first place that the truth of Dickson's conjecture can be established without assuming Weil's theorem. It suffices to use instead some results due to Davenport [3]; the value of N_k found in this way is somewhat poorer.

Since it is no more difficult we consider the following more general problem. Let e denote a fixed divisor of $p^n - 1$, where now the case $p = 2$ is included. Let $F(x) \in GF[p^n, x]$ and let $F(a) = b^e$, where $b \in GF(p^n)$ for all $a \in GF(p^n)$; the value $b = 0$ may be allowed. We may evidently assume that $F(x) \neq cH^e(x)$, where $c \in GF(p^n)$, $H(x) \in GF[p^n, x]$.

We now define a complex-valued function $\chi(M)$ for $M \in GF[p^n, x]$. Consider first the congruence

$$U^{p^n-1} \equiv F \pmod{P} \qquad (P \nmid F), \tag{1.1}$$

where P is irreducible and define $\{F/P\}$ as the number of $GF(p^n)$ such that

$$\{F/P\} \equiv F^{(p^{nh}-1)/(p^n-1)} \pmod{P} \qquad (\deg P = h).$$

Thus (1.1) is solvable if and only if $\{F/P\} = 1$. If next $M = P_1 \cdots P_r$, we put

$$\{F/M\} = \{F/P_1\} \cdots \{F/P_r\}.$$

Let γ denote a primitive root of $GF(p^n)$ and put $\{F/M\} = \gamma^r$. We then define $\chi(M) = e^{2\pi irf/(p^n-1)}$, where $ef = p^n - 1$; to complete the definition we put $\chi(M) = 0$ for $(M, F) \neq 1$. If we next put

$$L(s, \chi) = \sum_M \chi(M) \mid M \mid^{-s} \qquad (\mid M \mid = p^{n \deg M}), \tag{1.2}$$

Received January 7, 1952.